In the claims:

Following is a complete set of claims as amended with this Response.

1. (Currently Amended) A method performed by a user terminal of a wireless access network, the method comprising:

obtaining a time reference from an access point of the wireless access network;

receiving a digital certificate issued by a certificate authority from the access point;

requesting certification of the time reference by a trusted entity;

receiving certification of the time reference by sending a message used to authenticate the user terminal to the access point, the message containing a timestamp based on the time reference, an identification of the trusted entity by which certification is to be performed, and a list of trusted entities by which certification may be performed; and

validating the digital certificate.

2. (Canceled)

3. (Canceled)

4. (Currently Amended) The method of claim 1 ~~claim 2~~, wherein receiving certification of the time reference comprises receiving a message from the access point, the message being signed by the trusted entity and containing information to verify the timestamp.

5. (Original) The method of claim 1, wherein requesting certification of the time reference comprises sending a message to the trusted entity, the message containing a timestamp and a request to compare the timestamp to a local time of the trusted entity.

6. (Previously Presented) The method of claim 1, wherein the digital certificate has a validity period, and wherein validating the access point comprises determining whether the validity period has expired using the certified time reference.

7. (Original) The method of claim 1, wherein the time reference comprises an absolute frame number.

8. (Currently Amended) A user terminal comprising:

a clock to maintain a time reference obtained from an access point;

a transmitter to send a request for certification of the time reference by a trusted entity by sending a message used to authenticate the user terminal to the access point, the message containing a timestamp based on the time reference maintained by the clock, an identification of the trusted entity by which certification is to be performed, and a list of trusted entities by which certification may be performed;

a receiver to receive the certification of the time reference and a digital certificate issued by a certificate authority from the access point; and

a processor coupled to the receiver to validate the digital certificate.

9. (Canceled)

10. (Canceled)

11. (Currently Amended) The user terminal of claim 8 ~~claim 9~~, wherein the user terminal receives the certification of the time reference by receiving a message from the access point, the message being signed by the trusted entity and containing information to verify the timestamp.

12. (Original) The user terminal of claim 8, wherein the user terminal requests certification of the time reference by sending a message to the trusted entity, the message containing a timestamp based on the time reference maintained by the clock and a request to compare the timestamp to a local time of the trusted entity.

13. (Previously Presented) The user terminal of claim 8, wherein the digital certificate has a validity period and wherein the user terminal validates the access point by determining whether the validity period has expired using the certified time reference.

14. (Original) The user terminal of claim 8, wherein the time reference comprises an absolute frame number.

15. (Currently Amended) A method performed by an access point of a wireless access network, the method comprising:

receiving a message including a timestamp from a user terminal of the wireless access network, a request that the timestamp be certified by the trusted entity, and an identification of the trusted entity; wherein the identification of the trusted entity comprises a list of entities trusted by the user terminal;

authenticating the user terminal using the message;

sending a request for certification of the timestamp to a trusted entity that is trusted by the user terminal;

receiving a time certification message signed by the trusted entity including a verification of the timestamp; and

sending the time certification message to the user terminal.

16. (Canceled)

17. (Canceled)

18. (Original) The method of claim 15, wherein sending a request for certification of the timestamp comprises forwarding the timestamp to the trusted entity so that the trusted entity can compare the timestamp to a local time of the trusted entity.

19. (Currently Amended) An access point comprising:

a receiver to receive a message including a timestamp from a user terminal, the received message further including a request that the timestamp be certified by the trusted entity and an identification of the trusted entity, the identification of the trusted entity comprising a list of entities trusted by the user terminal;

a processor coupled to the receiver to authenticate the user terminal based on the received message; and

a transmitter coupled to the processor, to send a request for certification of the timestamp to a trusted entity that is trusted by the user terminal, and to forward a certification message received from and signed by the trusted entity, the certification message including a verification of the timestamp.

20. (Canceled)

21. (Canceled)

22. (Original) The access point of claim 19, wherein the transmitter further forwards the timestamp to the trusted entity so that the trusted entity can compare the timestamp to a local time of the trusted entity.

23. (Currently Amended) A machine-readable medium storing data representing instructions that, when executed by a processor of a user terminal, cause the processor to perform operations comprising:

obtaining a time reference from an access point:

receiving a digital certificate issued by a certificate authority from the access point;

requesting certification of the time reference by a trusted entity by sending a message used to authenticate the user terminal to the access point, the message containing a timestamp based on the time reference, an identification of the trusted entity by which certification is to be performed, and a list of trusted entities by which certification may be performed;

receiving certification of the time reference; and

validating the digital certificate.

24. (Canceled)

25. (Canceled)

26. (Currently Amended) The machine-readable medium of claim 23 ~~claim 24~~, wherein receiving certification of the time reference comprises receiving a message from the access point, the message being signed by the trusted entity and containing information to verify the timestamp.

27. (Original) The machine-readable medium of claim 23, wherein requesting certification of the time reference comprises sending a message to the trusted entity, the message containing a timestamp and a request to compare the timestamp to a local time of the trusted entity.

28. (Previously Presented) The machine-readable medium of claim 23, wherein the digital certificate has a validity period, and wherein validating the access point comprises determining whether the validity period has expired using the certified time reference.

29. (Original) The machine-readable medium of claim 23, wherein the time reference comprises an absolute frame number.

30. (Currently Amended) A machine-readable medium storing data representing instructions that, when executed by a processor of an access point, cause the processor to perform operations comprising:

receiving a message including a timestamp from a user terminal, the message further including a request that the timestamp be certified by the trusted entity and an identification of the trusted entity, wherein the identification of the trusted entity comprises a list of entities trusted by the user terminal;

authenticating the user terminal using the message;

sending a request for certification of the timestamp to a trusted entity that is trusted by the user terminal;

receiving a time certification message signed by the trusted entity including a verification of the timestamp; and

sending the time certification message to the user terminal.

31. (Canceled)

32. (Canceled)

33. (Original) The machine-readable medium of claim 30, wherein sending a request for certification of the timestamp comprises forwarding the timestamp to the trusted entity so that the trusted entity can compare the timestamp to a local time of the trusted entity.

34. (New) A method performed by a user terminal of a wireless access network, the method comprising:

obtaining a time reference from an access point of the wireless access network;

receiving a digital certificate issued by a certificate authority from the access point;

requesting certification of the time reference by a trusted entity by sending a message used to authenticate the user terminal to the access point, the message containing a timestamp based on the time reference and an identification of the trusted entity by which certification is to be performed;

receiving certification of the time reference by receiving a message from the access point, the message being signed by the trusted entity and containing information to verify the timestamp; and

validating the digital certificate.

35. (New) The method of claim 34, wherein the message contains a list of trusted entities by which certification may be performed.

36. (New) The method of claim 34, wherein requesting certification of the time reference comprises sending a message to the trusted entity, the message containing a timestamp and a request to compare the timestamp to a local time of the trusted entity.

37. (New) The method of claim 34, wherein the digital certificate has a validity period, and wherein validating the access point comprises determining whether the validity period has expired using the certified time reference.

38. (New) The method of claim 34, wherein the time reference comprises an absolute frame number.

39. (New) A user terminal comprising:

a clock to maintain a time reference obtained from an access point;

a transmitter to send a request for certification of the time reference by a trusted entity by sending a message used to authenticate the user terminal to the access point, the message containing a timestamp based on the time reference maintained by the clock and an identification of the trusted entity by which certification is to be performed;

a receiver to receive the certification of the time reference and a digital certificate issued by a certificate authority from the access point by receiving a message from the access point, the message being signed by the trusted entity and containing information to verify the timestamp; and

a processor coupled to the receiver to validate the digital certificate.

40. (New) The user terminal of claim 39, wherein the message contains a list of trusted entities by which certification may be performed.

41. (New) The user terminal of claim 39, wherein the user terminal requests certification of the time reference by sending a message to the trusted entity, the message containing a timestamp based on the time reference maintained by the clock and a request to compare the timestamp to a local time of the trusted entity.

42. (New) The user terminal of claim 39. wherein the digital certificate has a validity period and wherein the user terminal validates the access point by determining whether the validity period has expired using the certified time reference.

43. (New) The user terminal of claim 39, wherein the time reference comprises an absolute frame number.